日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

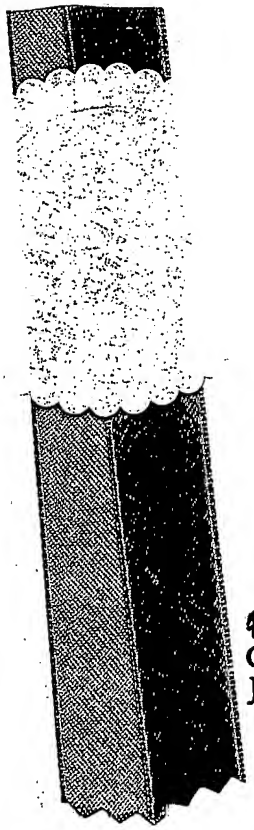
This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ３月 ２日

出願番号
Application Number: 特願２００１－０５９０４２

[ST.10/C]: [ＪＰ２００１－０５９０４２]

出願人
Applicant(s): セイコーエプソン株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT

２００２年 １月１１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３１１４１７８

【書類名】　特許願
【整理番号】　J0083370
【提出日】　平成13年 3月 2日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
　【氏名】　山門　均
【特許出願人】
　【識別番号】　000002369
　【氏名又は名称】　セイコーエプソン株式会社
【代理人】
　【識別番号】　100093388
　【弁理士】
　【氏名又は名称】　鈴木　喜三郎
　【連絡先】　０２６６－５２－３１３９
【選任した代理人】
　【識別番号】　100095728
　【弁理士】
　【氏名又は名称】　上柳　雅誉
【選任した代理人】
　【識別番号】　100107261
　【弁理士】
　【氏名又は名称】　須澤　修
【手数料の表示】
　【予納台帳番号】　013044
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9711684

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置及び当該情報処理装置の制御方法、並びに制御プログラム及び当該制御プログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項１】　固有の識別データを無線送信する可搬操作子と、

前記可搬操作子によって操作され、該操作を検出すると検出結果を出力する操作検出手段と、

識別データを記録する記録手段と、

前記可搬操作子から送信される識別データを受信する受信手段と、

前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手段と、

前記判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手段と、

前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段と

を備えることを特徴とする情報処理装置。

【請求項２】　固有の識別データを無線送信する可搬操作子と、

前記可搬操作子によって操作され、該操作を検出すると検出結果を出力する操作検出手段と、

ユーザデータと識別データを記録する記録手段と、

前記可搬操作子から送信される識別データを受信する受信手段と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手段と、

前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手段と、

前記第１の判定手段により該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られた

と判定する認証手段と、

前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段と

を備えることを特徴とする情報処理装置。

【請求項３】　可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、

前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を有することを特徴とする情報処理装置の制御方法。

【請求項４】　可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手順と、

前記第１の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を有することを特徴とする情報処理装置の制御方法。

【請求項５】　可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、

前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を実行させるための制御プログラム。

【請求項６】　可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手順と、

前記第１の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を実行させるための制御プログラム。

【請求項７】　可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、

前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を実行させるための制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項８】　可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手順と、

前記第１の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を実行させるための制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置に関し、ユーザの認証を行う情報処理装置に関する。

【０００２】

【従来の技術】

従来、パーソナルコンピュータやワークステーション等の情報処理装置においては、ログイン等の際にユーザ名とパスワードに基づいてユーザ認証を行っている。近年では、ユーザ名とパスワードに限らず、指紋などの生体情報を用いてユーザ認証を行う方法も提案されている。

【０００３】

【発明が解決しようとする課題】

しかしながら、この種の情報処理装置においては、一端ユーザ認証が得られると、明示的にログアウトまたは電源がオフされるまでは誰でも使用できる状態となってしまう。このため、正規のユーザがログアウトせずに情報処理装置から離れた場合は、第三者に不正利用されるおそれがあった。

【０００４】

また、ユーザ名とパスワードのみでユーザの認証を行う場合は、第三者にユーザ名とパスワードが知られてしまうと、正規のユーザに知られることなく第三者が正規のユーザになりすますことができる問題がある。

これらの場合にユーザの認証を繰り返し行う方法も考えられるが、パスワードなどの入力作業や指紋認証処理を何度も行う必要があり、使い勝手が悪くなってしまう問題が生じる。

【０００５】

そこで本発明の目的は、簡易かつ確実に第三者の不正利用を防止することができる情報処理装置及び当該情報処理装置の制御方法、並びに制御プログラム及び該制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的としている。

【０００６】

【課題を解決するための手段】

上記課題を解決するため、本発明は、固有の識別データを無線送信する可搬操作子と、前記可搬操作子によって操作され、該操作を検出すると検出結果を出力

する操作検出手段と、識別データを記録する記録手段と、前記可搬操作子から送信される識別データを受信する受信手段と、前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手段と、前記判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手段と、前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段とを備えることを特徴としている。

【０００７】

この構成によれば、情報処理装置は、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【０００８】

また、本発明は、固有の識別データを無線送信する可搬操作子と、前記可搬操作子によって操作され、該操作を検出すると検出結果を出力する操作検出手段と、ユーザデータと識別データを記録する記録手段と、前記可搬操作子から送信される識別データを受信する受信手段と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手段と、前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手段と、前記第１の判定手段により該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手段と、前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段とを備えることを特徴としている。

【０００９】

この構成によれば、情報処理装置は、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否

かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【００１０】

また、本発明は、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを有することを特徴としている。

【００１１】

この構成によれば、情報処理装置は、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【００１２】

また、本発明は、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手順と、前記第１の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応

する処理を行う情報処理手順とを有することを特徴としている。

【００１３】

この構成によれば、情報処理装置は、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【００１４】

また、本発明は、制御プログラムにおいて、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【００１５】

このプログラムによれば、コンピュータは、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【００１６】

また、本発明は、制御プログラムにおいて、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手順と、前記第１の判定手順にお

いて該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【００１７】

このプログラムによれば、コンピュータは、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【００１８】

また、本発明は、コンピュータ読み取り可能な記録媒体において、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【００１９】

この記録媒体によれば、コンピュータは、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【００２０】

また、本発明は、コンピュータ読み取り可能な記録媒体において、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データ

を受信する受信手順と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第１の判定手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第２の判定手順と、前記第１の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第２の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【００２１】

この記録媒体によれば、コンピュータは、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【００２２】

【発明の実施の形態】

以下、適宜図面を参照しながら本発明の実施形態について説明する。

【００２３】

（１）　実施形態

（１．１）　実施形態の構成

図１は、本発明の実施形態に係る情報処理装置１とこの情報処理装置１の操作を行うペン型操作子２の外観を示す図である。ペン型操作子２は、操作者がペンのように手に持って用いるポインティングデバイスである。情報処理装置１は、ペン型操作子２を持った操作者が机の上において操作したり、バックにいれて持ち運んで外出先で使用する装置である。

【００２４】

情報処理装置１は、略矩形形状の薄型のボディを持ち、その表面には略全面にわたって表示画面３が設けられている。表示画面３は、図２に示すように、液晶

表示パネル３ａと、この液晶表示パネル３ａの上面に設けられる透明のタッチパネル（操作検出手段）３ｂを有しており、ペン型操作子２によって表示画面３の表面が押圧されると、その位置がタッチパネル３ｂにより検出されるようになっている。

【００２５】

次に、図３を参照して、情報処理装置１とペン型操作子２の電気的構成を説明する。

情報処理装置１において、ＣＰＵ（判定手段、情報処理手段）１０は、ＲＯＭ１２に記録されたプログラムを読み出して実行することにより、この情報処理装置１全体の制御を行う。ＲＡＭ１１は、ＣＰＵ１０の制御の下に表示画面３に表示するイメージデータ等を一時的に格納するバッファメモリとして機能すると共に、各種データを一時記憶する。後述する処理に用いられる認証フラグＦもこのＲＡＭ１１に設定される。ＲＯＭ１２は、ＣＰＵ１０が読み出して実行する各種プログラムやペン型操作子２の識別データＩＤ等を記録するメモリである。フラッシュメモリ１３は、ＣＰＵ１０の制御の下に各種データを不揮発状態で保持するメモリである。液晶駆動部１４は、ＲＡＭ１１に記録されたイメージデータを読み出して対応する画像データを液晶表示パネル３ａに表示させる。受信部１５は、ＣＰＵ１０の制御の下にアンテナから入力したデータを受信し、受信データをＣＰＵ１０に出力する。入出力部１６は、ＣＰＵ１０の制御の下に入出力端子を介してインターネットに接続したり、パーソナルコンピュータ（ＰＣ）等と接続してデータ通信を行う。

【００２６】

次に、ペン型操作子２の電気的構成について説明する。ペン型操作子２において、メモリ２０は、固有の識別データＩＤを記録するメモリである。送信部２１は、メモリ２０に記録された識別データＩＤをアンテナ２ａ（図１参照）から無線で送信させる。ここで、ペン型操作子２の送信部２１と情報処理装置１の受信部１５との間の通信方式には、短距離無線通信方式が適用され、ペン型操作子２が情報処理装置１の近傍（例えば数ｍの範囲内）に存在する場合にのみ受信部１５が識別データＩＤを受信できるようになっている。この短距離無線通信方式に

は、例えば、マイクロ波方式、電磁誘導方式が適用され、変調方式には、スペクトラム拡散（Spread Spectrum）方式、周波数ホッピング（Frequency Hopping）方式または直接拡散（Direct Sequence）方式等が適用される。

【００２７】

（１．２）　実施形態の動作

次に、この情報処理装置１の概略動作を説明する。

まず、この情報処理装置１の初期設定時の動作を説明について説明する。

電源ボタンが操作されて情報処理装置１の電源が初めて投入されると、ＣＰＵ１０は、初期設定処理を行う。この初期設定処理においては、ＣＰＵ１０は、液晶駆動部１４により図４に示す登録画面３０を表示画面３に表示させ、操作者によりペン型操作子２で表示画面３が押圧操作されると、表示画面３のタッチパネル３ｂから通知される押圧位置に基づいてユーザ名とパスワードの登録処理を行う。

【００２８】

具体的には、ＣＰＵ１０は、押圧位置がユーザ名の入力欄３０ａまたはパスワードの入力欄３０ｂ内であると判定した場合は、各入力欄３０ａまたは３０ｂの対応する位置にカーソルを点滅させる。また、ＣＰＵ１０は、押圧位置が文字パレット３０ｃ内の文字等であると判定した場合は、その文字等を入力欄３０ａまたは３０ｂのカーソル点滅位置に表示させる一方、押圧位置が削除ボタン３０ｄであると判定した場合は、入力欄３０ａまたは３０ｂのカーソル点滅位置にある文字等を消去させる。さらに、ＣＰＵ１０は、押圧位置が登録ボタン３０ｅであると判定した場合は、各入力欄３０ａ及び３０ｂに入力されたユーザ名とパスワードをフラッシュメモリ１３に記録し、記録が終了すると、ユーザ名とパスワードの登録処理を終了する。

【００２９】

次に、図５に示すフローチャートを参照して、情報処理装置１のメインルーチンについて説明する。

まず、電源ボタンが操作されて情報処理装置１の電源が投入されると、ＣＰＵ１０は、初期化処理を行う（ステップＳ１）。この初期化処理において、ＣＰＵ

１０は、ＲＡＭ１１の予め定めた領域に認証フラグＦ＝［０］を設定する。この初期化処理が終了すると、ＣＰＵ１０は、液晶駆動部１４により操作画面４０を表示画面３に表示させる（ステップＳ２）。ここで、図６は、操作画面４０の一例を示す図である。

【００３０】

このとき、ＣＰＵ１０は、認証処理を開始し（ステップＳ３）、その後、操作者によりペン型操作子２で表示画面３が押圧操作され、タッチパネル３ｂから押圧位置が通知されると（ステップＳ４：YES）、ＲＡＭ１１に格納した認証フラグＦを参照する（ステップＳ５）。ここで、ＣＰＵ１０は、認証フラグＦが［０］の場合は、ステップＳ３に処理を戻すのに対し、認証フラグＦが［１］の場合は、タッチパネル３ｂから通知される押圧位置に基づいて対応する処理を行う（ステップＳ６）。

【００３１】

具体的には、認証フラグＦが［１］の場合、ＣＰＵ１０は、押圧位置が操作画面４０（図４参照）の作業エリア４０ａ内であると判定すると、液晶駆動部１４により押圧位置に対応する位置の液晶表示パネル３ａのドットを反転表示させ、押圧位置の軌跡を表示画面３に表示させる。また、ＣＰＵ１０は、押圧位置が操作画面４０内のいずれかの操作ボタン４０ｂであると判定した場合は、その操作ボタン４０ｂに対応する処理を行う。例えば、押圧位置が「スケジューラ」ボタン４０ｂの場合は、ＣＰＵ１０は、「スケジューラ」ボタン４０ｂを反転表示させると共に、作業エリア４０ａにスケジュール画面を表示させる。

そして、ＣＰＵ１０は、タッチパネル３ｂから通知される押圧位置に基づいて対応する処理を行うと、ステップＳ３の処理に戻す。このように、ＣＰＵ１０は、ステップＳ３～Ｓ６までの処理を電源がオフされるまで繰り返し、操作者によりペン型操作子２で表示画面３が押圧操作される毎に認証フラグＦを参照し、認証フラグＦに応じて対応する処理を行うか否かを選択するようになっている。

【００３２】

次に、図７及び図８に示すフローチャートを参照して、認証処理について説明する。

まず、ＣＰＵ１０は、情報処理装置１の電源投入後、液晶駆動部１４によりログイン画面５０を表示画面３に表示させる（ステップＳ１０）。図９は、ログイン画面５０の一例を示す図である。次に、ＣＰＵ１０は、タッチパネル３ｂから押圧位置が通知されると（ステップＳ１１：YES）、押圧位置がログインボタン５０ｅであるか否かを判定する（ステップＳ１２）。ここで、ログイン画面５０は、「ログイン」ボタン５０ｅを有する点を除いて登録画面３０（図４参照）とほぼ同一であるため、同一の部分は同一の符号を付して示している。すなわち、ＣＰＵ１０は、押圧位置が「ログイン」ボタン５０ｅ以外の位置の場合は、登録画面３０の場合と同様の処理を行う（ステップＳ１３）。操作者は、上述した登録画面３０の場合と同様にして入力欄３０ａ及び入力欄３０ｂにユーザ名とパスワードを入力する。

【００３３】

一方、ＣＰＵ１０は、押圧位置がログインボタン５０ｅであると判定した場合は（ステップＳ１２：YES）、入力されたユーザ名とパスワードがフラッシュメモリ１３に記録されたユーザ名とパスワードと一致するか否かを判定する（ステップＳ１４）。この判定において、一致しないと判定された場合は（ステップＳ１４：NO）、ＣＰＵ１０は、ステップＳ１１の処理に戻す。これに対して、入力されたユーザ名とパスワードがフラッシュメモリ１３に記録されたものと一致すると判定した場合は（ステップＳ１４：YES）、ＣＰＵ１０は、受信部１５に受信開始を指示する（ステップＳ１５）。

【００３４】

次に、ＣＰＵ１０は、受信部１５の受信結果に基づいて識別データＩＤ（以下、受信した識別データＩＤを「識別データＩＤａ」という。）を受信したか否かを判定し（ステップＳ１６）、識別データＩＤａを受信したと判定した場合は（ステップＳ１６：YES）、受信した識別データＩＤａがＲＯＭ１４に記録された識別データＩＤと一致するか否かを判定する（ステップＳ１７）。

【００３５】

ここで、ＣＰＵ１０は、識別データＩＤａを受信しなかったと判定した場合（ステップＳ１６：NO）若しくは受信した識別データＩＤａがＲＯＭ１４に記録さ

れた識別データＩＤと一致しなかった場合は（ステップＳ１７：NO）、認証が得られないとして認証フラグＦを［１］に設定する（ステップＳ１８）。そして、ＣＰＵ１０は、認証フラグＦを［１］に設定するとステップＳ１６に処理を戻す。

一方、ＣＰＵ１０は、ステップＳ１７において、受信した識別データＩＤａがＲＯＭ１４に記録された識別データＩＤと一致すると判定した場合は、認証が得られたとして認証フラグＦを［０］に設定する（ステップＳ１９）。 そして、ＣＰＵ１０は、認証フラグＦを［０］に設定すると、ステップＳ１６に処理を戻す。

【００３６】

以上のようにして、ＣＰＵ１０は、ステップＳ１６→Ｓ１７→Ｓ１９→Ｓ１６という処理か、ステップＳ１６→（Ｓ１７）→Ｓ１８→Ｓ１６という処理のいずれかを行う。これらの循環処理は、ＣＰＵ１０の処理速度からすれば、極めて速い循環処理になり、受信の有無の判断（ステップＳ１６）および識別データの比較処理（ステップＳ１７）は、実質的に継続して行われるのと同等となる。すなわち、上記の循環処理により、電源が投入された後はＣＰＵ１０により、受信部１５が受信した識別データＩＤａとＲＯＭ１２に記憶された内容との一致が継続的に判断される。

【００３７】

このように、本願においては、使用に際して最初だけ判定するのではなく、実質的な意味で継続的に判定をしている。このため、この情報処理装置１は、正規のユーザが使用するペン型操作子２が情報処理装置１の近くに存在する間だけタッチパネル３ｂを介して入力したユーザの操作に対応する処理を行うことができる。従って、この情報処理装置１は、正規のユーザが装置から離れた場合などは、即座にその状況を検出することができ、不正使用者による入力を防止することができると共に、正規のユーザが装置の近くに戻ってくればすぐに使用を開始することができる。

【００３８】

また、この情報処理装置１は、ペン型操作子２が近くにあれば使用できるので

、ペン型操作子２を持った正規のユーザが近くにいれば、他のペン型操作子を用いても使用することができる。従って、例えば、正規のユーザがその場で第三者に情報処理装置１を渡して第三者のペン型操作子を使って電話番号を入力してもらうといったことも従来機器と同様に行うことができる。すなわち、正規のユーザは、自分のペン型操作子２を身近に持っておけば、第三者の不正利用を確実に防止できるのである。

【００３９】

（２）　本願発明は、上述した実施形態に限らず種々の態様にて実施することができる。例えば、以下のような変形実施が可能である。

（２．１）

上述の実施形態においては、ＣＰＵ１０の処理速度により識別データの受信判定と識別データの比較判定とが継続して行われるようにしたが、比較判定については、例えば、タイマ等を設け、このタイマの出力に同期して数秒おきに判定するようにしてもよい。

（２．２）

上述の本実施形態においては、ＣＰＵ１０による認証の判定を所定間隔で行うようにしている。この場合、受信部１５の受信動作を判定が行われるタイミングだけにすれば、消費電力の点で有利である。すなわち、受信部１５に間欠駆動受信を行わせ、この間欠駆動のタイミングとＣＰＵ１０による判定のタイミングを同期させるように構成してもよい。

（２．３）

上述の実施形態においては、プログラムに基づくＣＰＵ１０の処理によって識別データの比較判定を行った。これに対し、図１０に示すように、識別データＩＤを記憶するレジスタ１００と、受信した識別データＩＤａが転送されるレジスタ１０１を設け、これらのレジスタ１００及び１０１の内容を比較するデジタルコンパレータ１０２によって、一致不一致を判定してもよい。すなわち、本発明の実施は、ソフトウエア処理によるばかりでなく、ハードウエアによっても実現することができる。

（２．４）

上述の実施形態では、入力されたユーザ名とパスワード、及び受信した識別データＩＤに基づいて認証を行ったが、識別データＩＤのみに基づいて認証を行ってもよい。

【００４０】

（２．５）

上述の実施形態では、ペン型操作子２が継続して識別データを送信していたが、ペン型操作子２に受信部を設けると共に情報処理装置１に送信部を設けて、ペン型操作子２が、情報処理装置１から送信された識別データＩＤの送信要求を受信した場合のみ識別データＩＤを送信するようにしてもよい。この場合、ペン型操作子２の平均消費電力を小さくできるので、ペン型操作子２の駆動時間を長くすることができる。

【００４１】

（２．６）

上述の実施形態では、ペン型操作子２を用いて操作する情報処理装置に本発明を適用する場合について述べたが、要は、可搬操作子を用いて操作する情報処理装置であれば本発明を適用でき、タブレットやマウス等で操作する情報処理装置でもよい。なお、本発明は、セキュリティーの観点から可搬操作子をユーザが携帯することが望ましいので、可搬操作子はコードレスの方がよい。また、本発明を適用できる情報処理装置には、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistants）等のプログラムを実行可能なコンピュータを含む。

【００４２】

（２．７）

上述の実施形態においては、認証処理を行うプログラムを予め情報処理装置１に記憶しておく場合について述べたが、図１１に示すように、この認証プログラムを磁気記録媒体、光記録媒体、半導体記憶媒体などのコンピュータが読み取り可能な記録媒体に記録し、コンピュータが認証プログラムを読み取って実行するようにしてもよい。また、図１２に示すように、この認証プログラムをサーバに格納し、ネットワークを介してサーバが送信要求のあったＰＣなどの端末に認証プログラムを送信するようにしてもよい。

【００４３】

【発明の効果】

上述したように本発明は、正規のユーザが使用する可搬操作子から送信される識別データに基づいて情報処理装置の近くに正規のユーザが存在するか否かを継続的に判定することにより、簡易かつ確実に第三者の不正利用を防止することができる。

【図面の簡単な説明】

【図１】　本発明の実施形態に係る情報処理装置とペン型操作子の外観を示す図である。

【図２】　情報処理装置の表示画面の構成を示す図である。

【図３】　情報処理装置とペン型操作子の電気的構成を示すブロック図である。

【図４】　情報処理装置が表示する登録画面の一例を示す図である。

【図５】　情報処理装置のメインルーチンのフローチャートである。

【図６】　情報処理装置が表示する操作画面の一例を示す図である。

【図７】　情報処理装置の認証処理の一部のフローチャートである。

【図８】　情報処理装置の認証処理の一部のフローチャートである。

【図９】　情報処理装置が表示するログイン画面の一例を示す図である。

【図１０】　変形実施例の説明に供する図である。

【図１１】　変形実施例の説明に供する図である。

【図１２】　変形実施例の説明に供する図である。

【符号の説明】

１……情報処理装置、

２……ペン型操作子、

２ａ……アンテナ、

３……表示画面、

３ａ……液晶表示パネル、

３ｂ……タッチパネル

１０……ＣＰＵ、

１１……ＲＡＭ

１２……ＲＯＭ、

１３……フラッシュメモリ、

１４……液晶駆動部、

１５……受信部、

１６……入出力部、

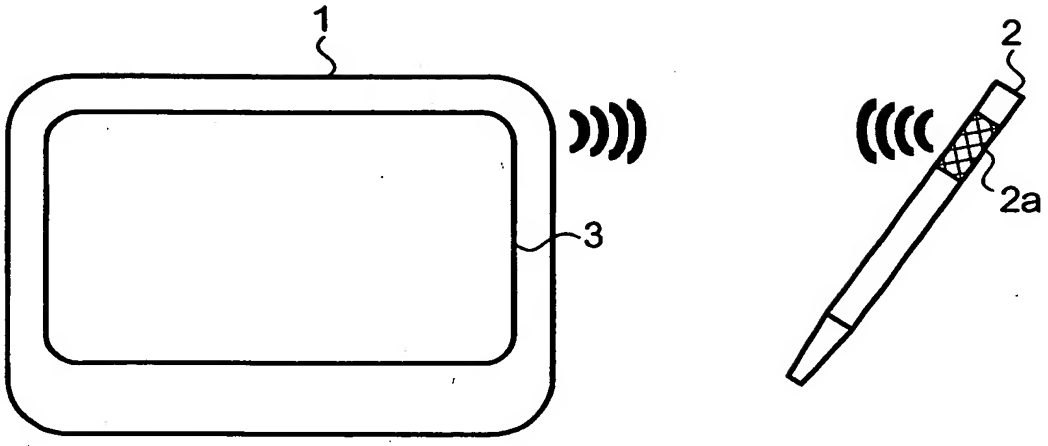
２０……メモリ、

２１……送信部、

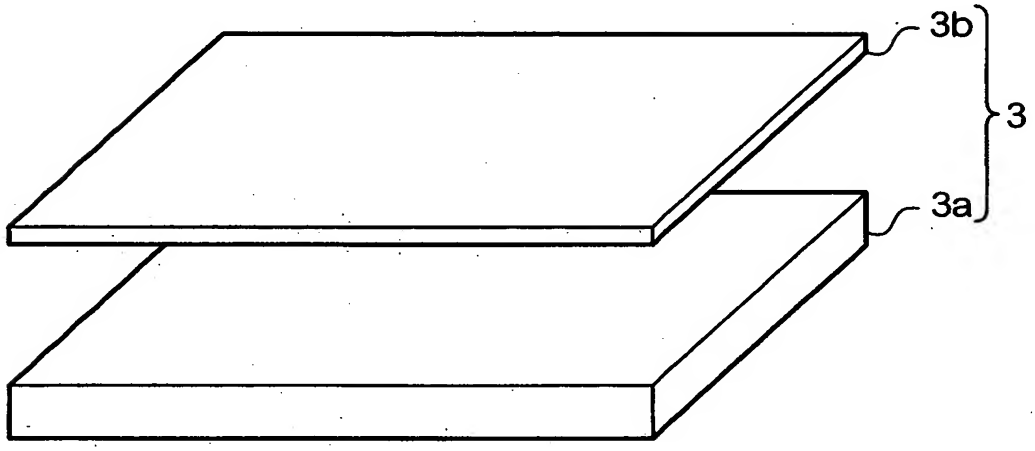
Ｆ……認証フラグ。

【書類名】　　図面

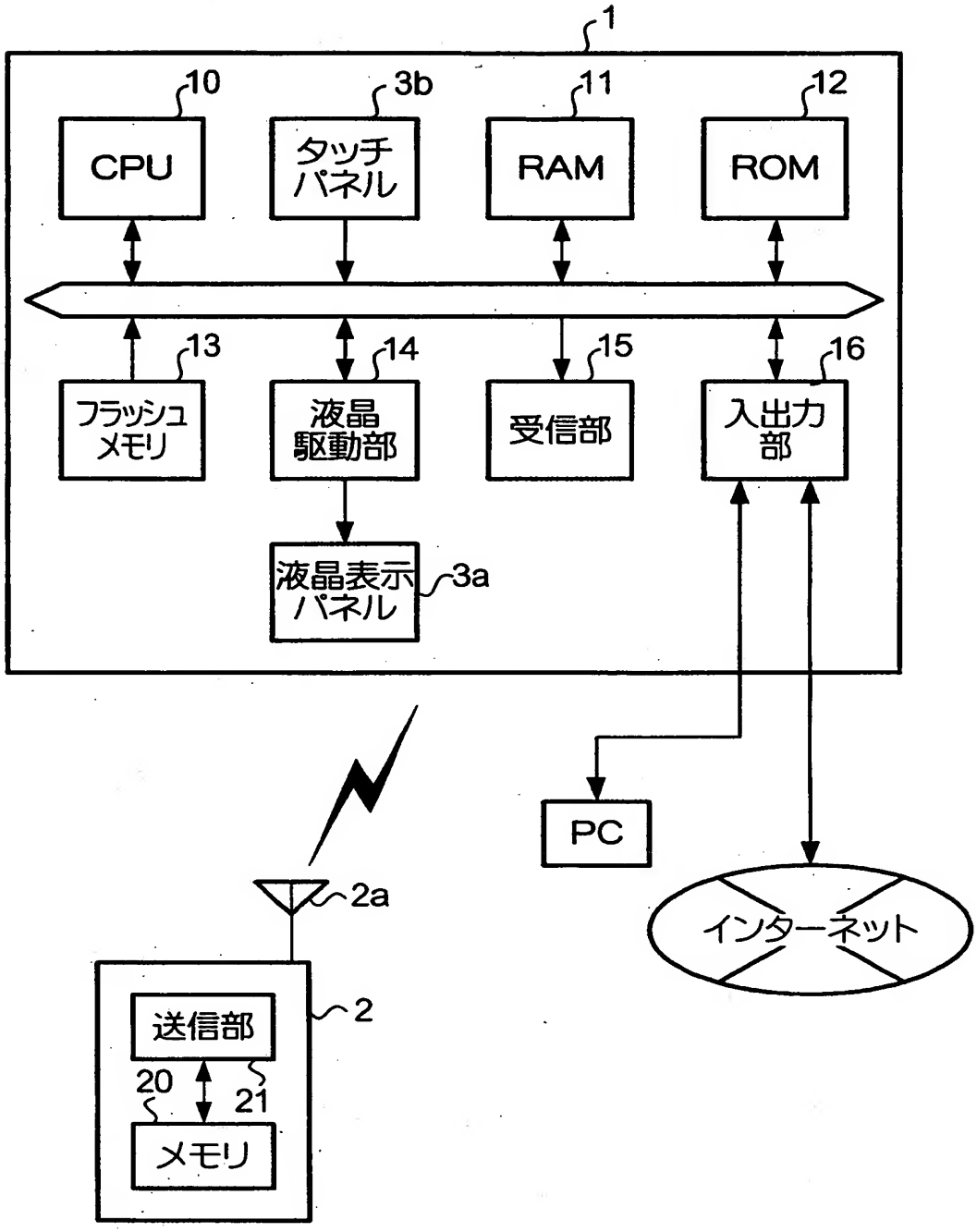
【図１】



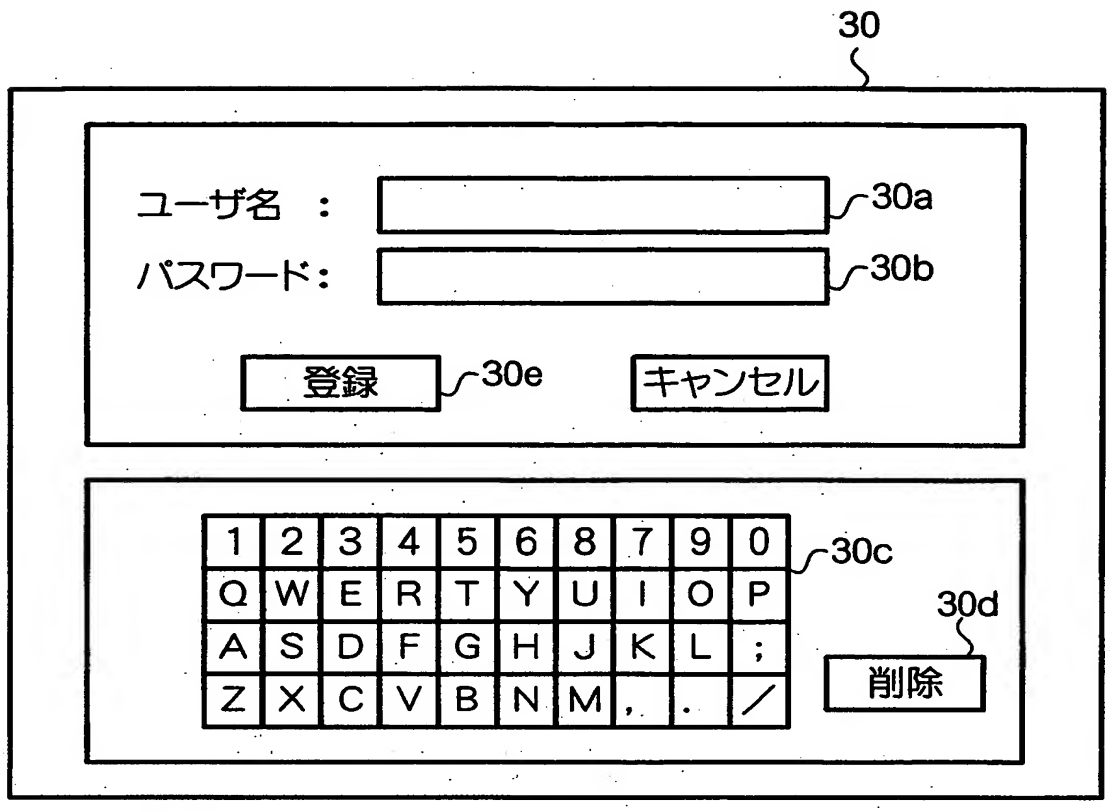
【図２】



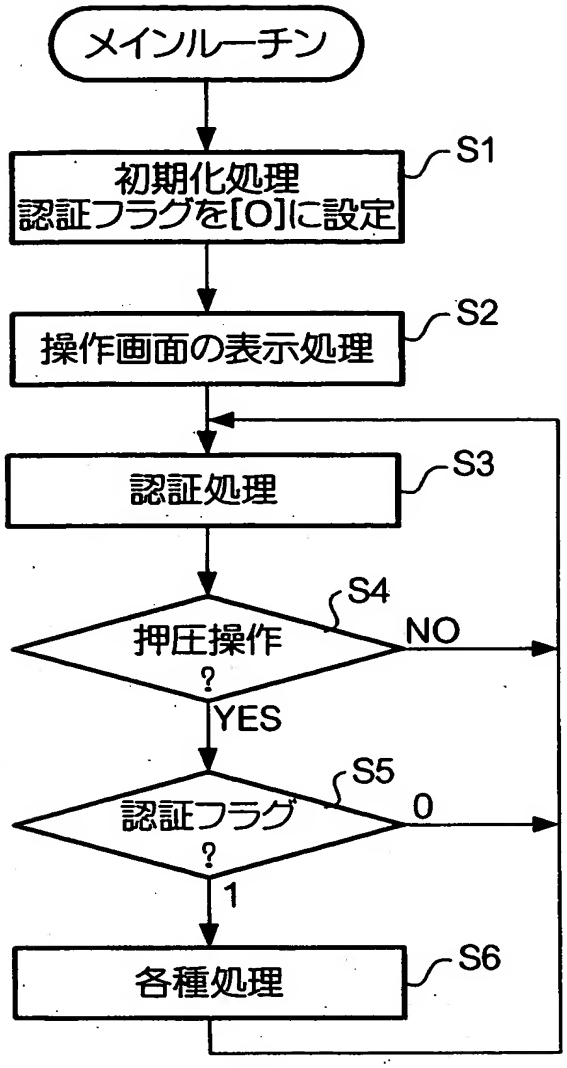
【図３】


1
10
CPU
3b
タッチパネル
11
RAM
12
ROM
13
フラッシュメモリ
14
液晶駆動部
15
受信部
16
入出力部
液晶表示パネル
3a
PC
インターネット
2a
2
送信部
20
21
メモリ

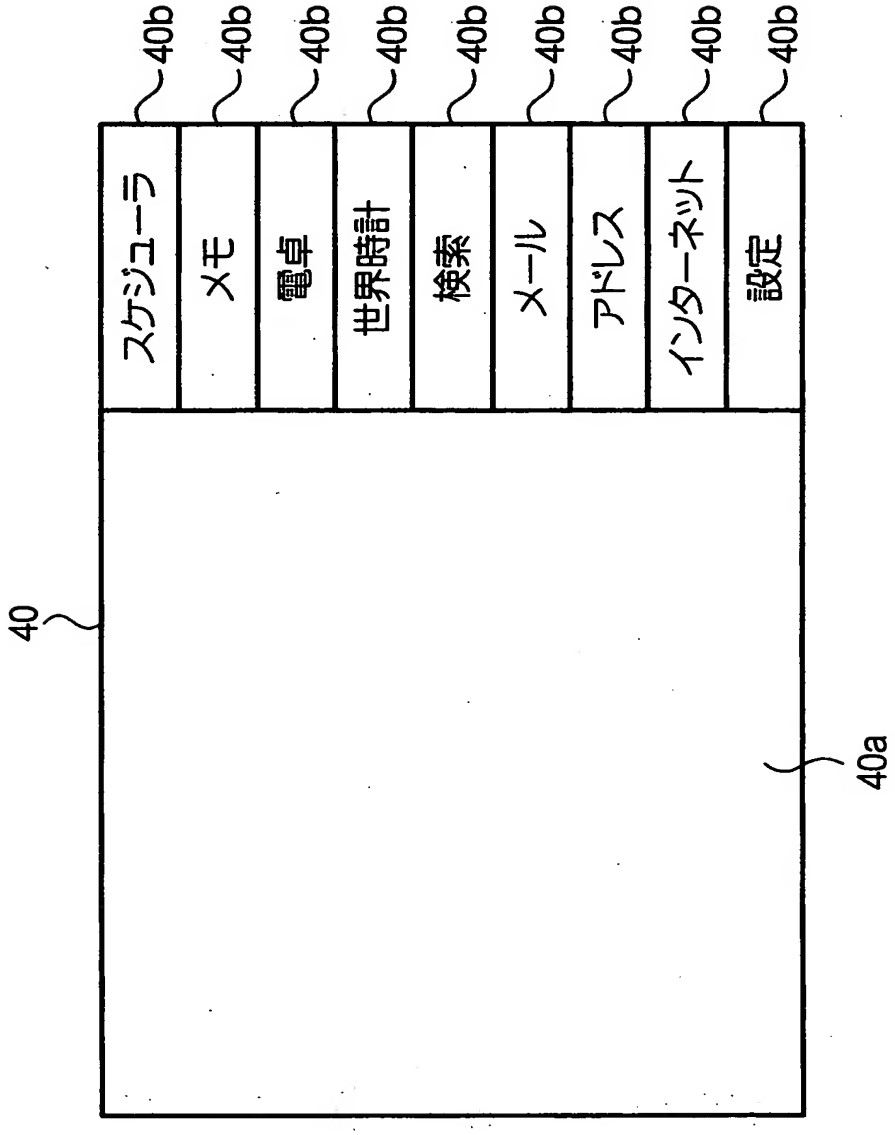
【図４】


30
ユーザ名 ：
30a
パスワード：
30b
登録
30e
キャンセル
1 2 3 4 5 6 8 7 9 0
Q W E R T Y U I O P
A S D F G H J K L ;
Z X C V B N M , . ／
30c
30d
削除

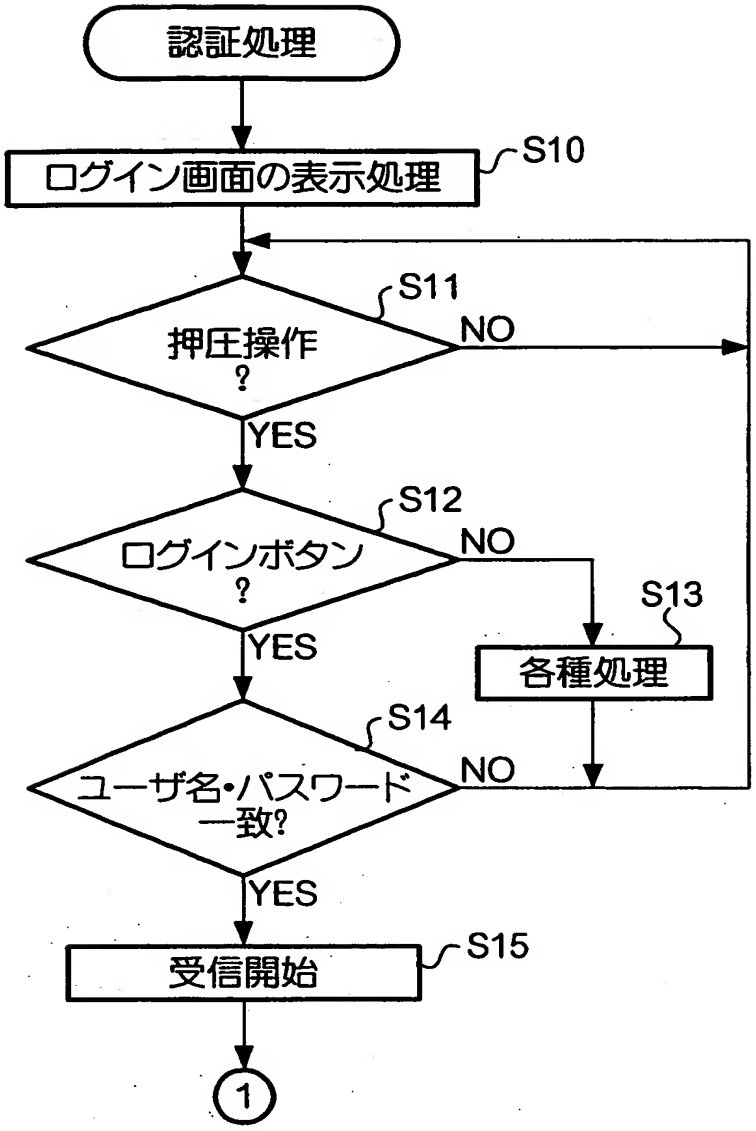
【図５】


メインルーチン
初期化処理
認証フラグを[0]に設定
S1
操作画面の表示処理
S2
認証処理
S3
押圧操作
?
S4
NO
YES
認証フラグ
?
S5
0
1
各種処理
S6

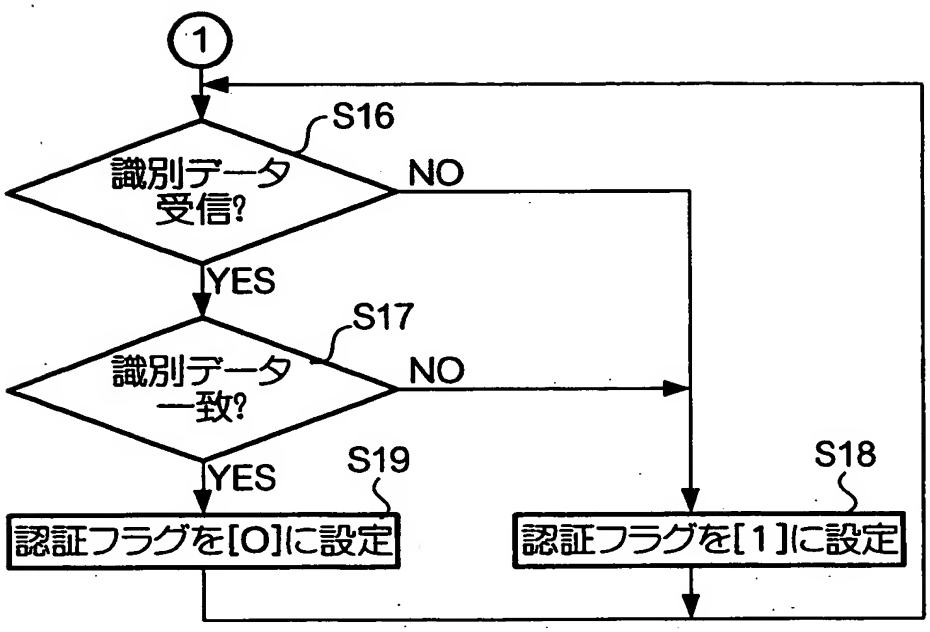
【図６】


40b
40b
40b
40b
40b
40b
40b
40b
40b
スケジューラ
メモ
電卓
世界時計
検索
メール
アドレス
インターネット
設定
40
40a

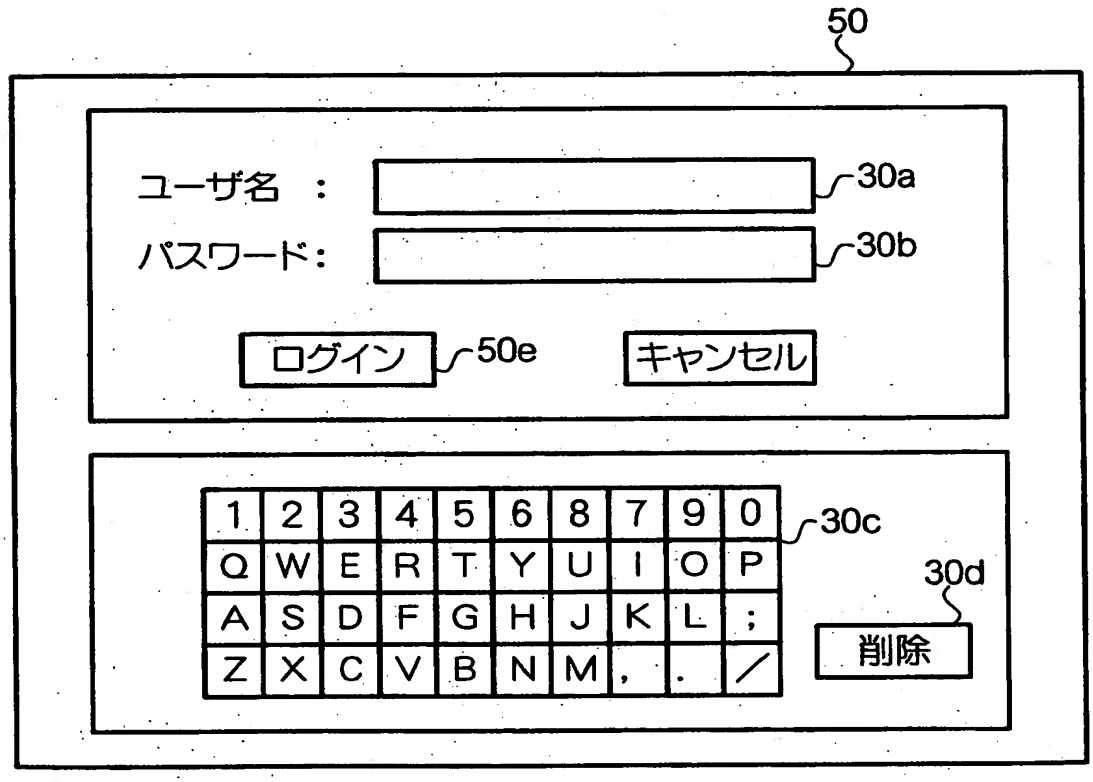
【図７】


認証処理
ログイン画面の表示処理
S10
S11
押圧操作
?
NO
YES
S12
ログインボタン
?
NO
S13
各種処理
YES
S14
ユーザ名・パスワード
一致?
NO
YES
受信開始
S15
1

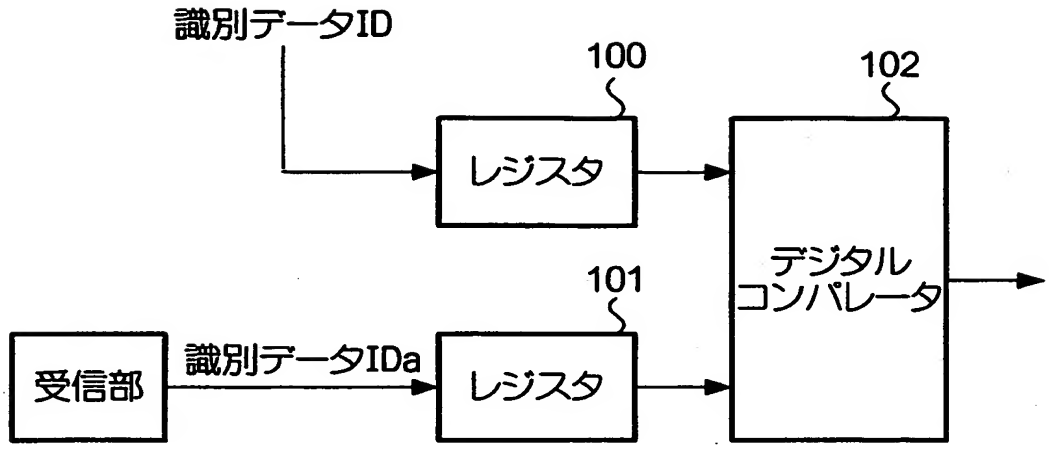
【図８】


1
S16
識別データ受信?
NO
YES
S17
識別データ一致?
NO
YES
S19
S18
認証フラグを[0]に設定
認証フラグを[1]に設定

【図９】


50
ユーザ名 ：
30a
パスワード:
30b
ログイン
50e
キャンセル
1 2 3 4 5 6 8 7 9 0
Q W E R T Y U I O P
A S D F G H J K L ;
Z X C V B N M , . /
30c
30d
削除

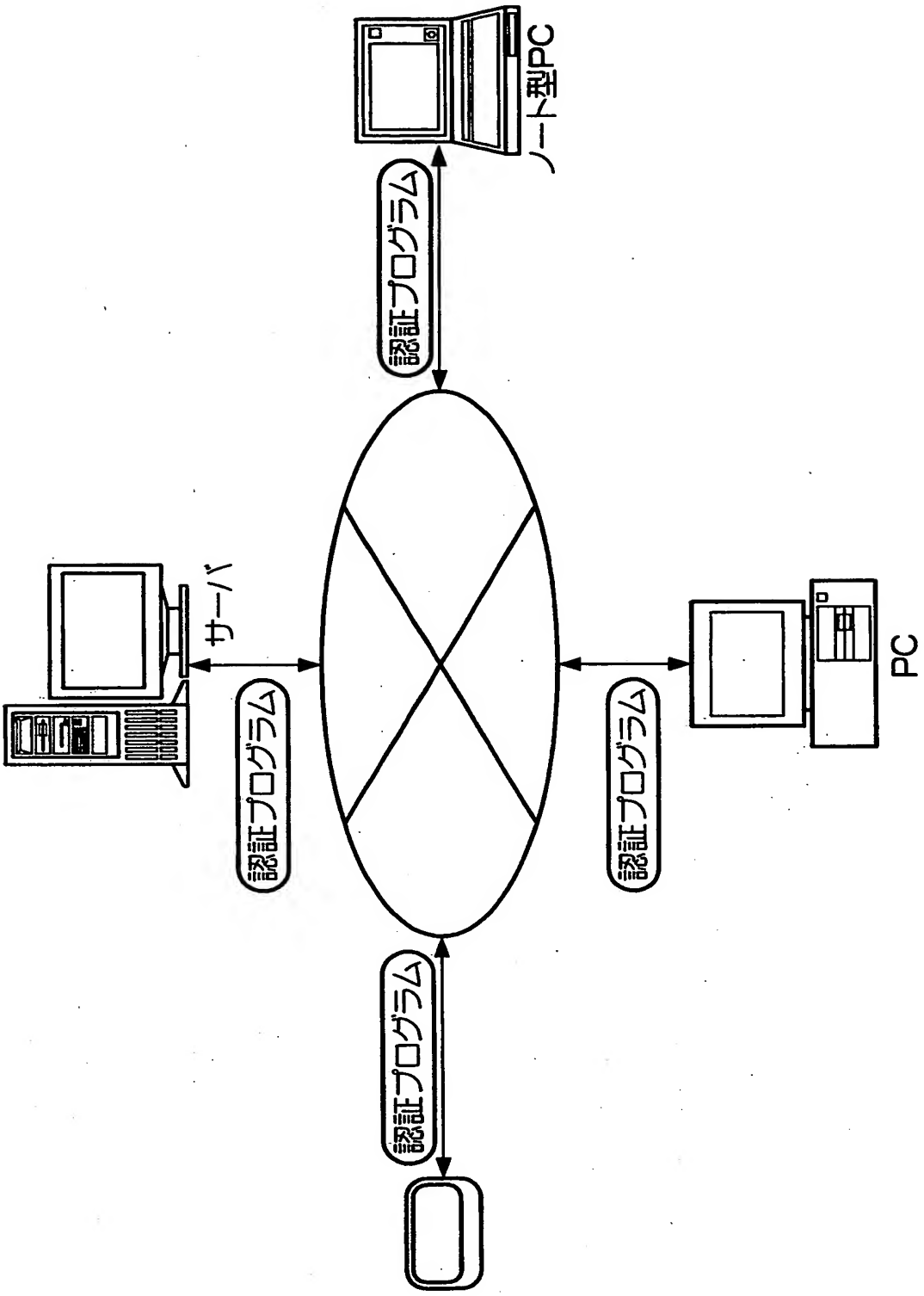
【図１０】


識別データID
100
102
レジスタ
デジタル
コンパレータ
101
受信部
識別データIDa
レジスタ

【図１１】


記録媒体
認証プログラム
コンピュータ

【図１２】



【書類名】　　要約書

【要約】

【課題】　簡易かつ確実に第三者の不正利用を防止することができる情報処理装置及び当該情報処理装置の制御方法、並びに制御プログラム及び当該制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【解決手段】　情報処理装置１は、正規のユーザが使用する可搬操作子２から送信される識別データＩＤに基づいて当該情報処理装置１の近くに正規のユーザが存在するか否かを継続的に判定し、該識別データＩＤを受信していると判定する間だけユーザの操作に対応する処理を行う。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２３６９〕

１．変更年月日　　１９９０年　８月２０日
［変更理由］　新規登録
住　所　　東京都新宿区西新宿２丁目４番１号
氏　名　　セイコーエプソン株式会社